Embracing the Cloud: Caveat Professor.

It has become a dominant meme to describe the role of information technology in higher education as transformative. We've all done it, myself included. My work as chief privacy and security officer at a large public university has, however, given me pause to ask if our posture toward risk prevents us from fully embracing technology at a moment of profound change.

There's no doubt that technology has radically transformed many, if not most, of our administrative processes. During my years at the University of Illinois at Urbana-Champaign, we've moved from paper-based processes to electronic workflows, Web portals and document repositories, and now mobile-device apps. How many of us, on either the academic or administrative side, can even imagine how we functioned before the advent of Google Apps, Skype, Dropbox, or arXiv.org.?

And technology marches on, faster than ever. Yet those of us with strategic responsibilities struggle to balance our institutional obligations and aversion to risk with the cold reality of the modern digital marketplace. In the eyes of our faculty and technologically savvy staff members, our internal-technology services must seem like dinosaurs--and not the cool, multicolored velociraptor of late, but the ponderous, stop-action brontosaurus of our youth. Consequently, faculty members are accepting major personal and institutional risk by using such third-party services without any institutional endorsement or support. How we provide those services requires a nuanced view of risk and goes to the heart of our willingness to trust our own faculty and staff members.

One can imagine a future in which the "where" of data storage is "everywhere," with a host of loosely coupled applications providing us services through any number of apps or interfaces. This is the world many of our users already live in. The technologically savvy among us recognize that hard physical, virtual, and legal boundaries actually demark this world of aggressively competitive commercial entities. Our students, faculty, and staff often do not.

Using applications built in the cloud--Dropbox, Google Docs, and Mozy, for example, which allow on-demand access to highly distributed and scalable Internet services--people on our campuses manage their friendships; business relationships; bank accounts, travel plans, and investments; and the collection of photos, videos, and other souvenirs of a life lived. Most recently, we've seen these same applications help topple entire governments.

But can we embrace the cloud? Can the faculty member who wears our institution's name in her title and e-mail address, to whom we've entrusted the academic and research mission of the institution, be trusted to reach into the cloud and pluck what she believes is the optimal tool to achieve her pedagogical aims and use it? Unfortunately, no. Many faculty and staff members simply use whatever service they choose, but they often do not have the knowledge or experience needed to evaluate those choices. And those who do try to work through the institution soon find themselves mired in bureaucracy.

For those not involved in this process, let me briefly describe what happens when a professor at Illinois approaches me about using a cloud service for teaching. First we review the company's terms of service. Of course, we also ask the company for any information it can provide on its internal data security and privacy practices. Our purchasing unit rewrites the agreement to include all of the state-required procurement language; we also add our standard contract language on data security.

All of this information is fed into some sort of risk assessment of varying degrees of formality, depending on the situation, and, frankly, the urgency. That leads to yet another round of modifications to the agreement, negotiations with the company, and, finally, if successful, circulation for signatures. After which we usually exhume the corpse of the long-deceased faculty member and give him approval to use the service in his class.

We go through this process not from misguided love of bureaucracy, but because our institutions know of no other way to manage risk. That is, we have failed to transform ourselves so we can thrive and compete in the 21st century.

Not only must we re-evaluate our attitude toward risk, but also our analysis of risk needs a paradigm shift. Particularly in the domain of information technology, we believe that control leads to minimized risk. By controlling an application (or a server or a network), a security officer can respond decisively when something goes wrong.

But our faculty and staff are increasingly voting with their feet--they're more interested in the elegance, portability, and integration of commercial offerings, despite the inability to control how those programs change over time. By insisting on remaining with homegrown solutions, we are failing to fall in lockstep with those we support.

Data security? Of course there are plenty of fly-by-night operations with terrible security practices. However, as the infrastructure market has matured (one of the generally unrecognized benefits of cloud services), more and more small companies can provide assurances of data security that would shame many of us even at large research-intensive institutions.

If higher education is to break free of the ossified practices of the past, we must find ways to transfer risk acceptance into the faculty domain--that is, to enable faculty to accept risk. Such a transformation is beyond the ability of the IT department alone--it will require our campus officials, faculty senates, registrars, and research and compliance officers working together to deeply understand both the risks and the benefits. I am not advocating a cavalier approach to the issues, but rather one that is deliberative and nuanced.

Here are a few of the characteristics we would expect to find in an ideal environment:

Greater transparency. Students deserve to be informed how their records and interactions with faculty and staff members are handled. We should be ashamed that Google is more transparent about how it uses our data than we are with our students.

Accessibility for those with special needs. Technology must be accessible to staff members and students who, for disability, safety, or privacy reasons, need special accommodations.

Better guidance. Professors would learn how to evaluate new tools and technologies through additional training. Winning a Nobel Prize doesn't prepare one to recognize that an online service tramples on its users' privacy.
More accountability. Embracing the freedom to accept risk means accepting responsibility for our actions. This is undoubtedly the most critical and difficult issue to resolve.

Every time a student uses an Internet-based service can be seen as an opportunity to educate. For instance, faculty members could provide students with a standardized outline of what services will be used during a

course, along with potential privacy risks and available protections. Surely such information could be included in course catalogs. Students would then be able to make informed decisions about needing accommodations or simply opting out. In some cases, students could be provided with opaque identifiers: identifying information that is known to the institution but is seen as anonymous avatars by the outside world.

Campus information-technology groups might need greater agility to respond to emerging technologies, including commercial offerings, and to help a much larger group of faculty members understand the risks of using these services.

All of this takes commitment and work, and accepting risk makes us personally and institutionally uncomfortable. But our colleges exist solely to advance the boundaries of human knowledge, and it's difficult to imagine any better place to challenge our sense of comfort.

~~~~~~~~

By MICHAEL CORN
Michael Corn is chief privacy and security officer at the University of Illinois at Urbana-Champaign.
~~~~~~~~